Email the completed PIA to
PIAteam@state.gov

DOS E-Mail Systems (Email) PIA

1. Contact Information

A/GIS/IPS Director
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

(a) Name of system: DOS Email Systems

(b) Bureau: Information Resource Management

(c) System acronym: Email

(d) iMatrix Asset ID Number: 737

(e) Reason for performing PIA

☐ New system

☒ Significant modification to an existing system

☐ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable) : New Security Controls Baselines released by NIST SP 800-53, Revision 4.

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?
☒Yes
☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system? The A&A process is in progress, estimated to be completed by the end of November 2016.

(c) Describe the purpose of the system:
The purpose of the system is to provide Sensitive But Unclassified (SBU) business communication via e-mail to Department of State employees and cleared contractors.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:
The system uses names and e-mail addresses and disseminates, with the potential to collect in users' mailboxes, other subject matter that could contain other examples of PII. For instance, Human Resources may retrieve SSNs and other personal information through disseminated attachments; Bureau security offices request badge ID numbers

from new hires; also temporary passwords (PINS) may be transmitted through the system.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?
Governing authorities that collect PII by way of email will be dependent on the functional authority of the office collecting the information.

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?
☐Yes, provide:
- SORN Name and Number:
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): Click here to enter a date.

☒No, explain how the information is retrieved without a personal identifier.
DoS Email Exchange does not collect PII. The governing offices/bureaus collecting the PII are responsible for ensuring they have appropriate SORN coverage and follow the appropriate procedures. Exchange is a tool that enables business communication by way of email, but it is not the record keeping system that manages, stores, files, correlates, amasses or identifies the records of business activity generated through email.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐Yes ☒No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☐Yes ☒No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov .)
Data maintained by Exchange serves different purposes for different business processes throughout the Department. Records retention and disposition vary by type of record collected. The record types will vary based on program needs. Information collected is maintained in accordance with data retention schedules appropriate to the specific activity and classification. Per the NARA directive emails classified as (Official – Privacy/PII) will be retained for seven years then deleted.

If yes provide:
- Schedule number (e.g., (XX-587-XX-XXX)): Click here to enter text.
- Length of time the information is retained in the system: Click here to enter text.
- Type of information retained in the system:
Click here to enter text.

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

☒ Members of the Public
☒ U.S. Government employees/Contractor employees
☒ Other (people who are not U.S. Citizens or LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☒Yes ☐No

- If yes, under what authorization?
Governing authorities that collect PII by way of email will be dependent on the functional authority of the office collecting the information.

(c) How is the information collected?
Exchange 15.x (the email system) does not collect information. Exchange 15.x only serves as a repository of the information collected by the governing authorities. Emails are sent/received from a user's email client (Outlook). When the email is sent/received it's uploaded to the SMTP (Simple Mail Transfer Protocol) server as outgoing/incoming email. The SMTP server locates the recipient's email server (Exchange) and transfers the email to their inbox which resides there indefinitely until deleted.

(d) Where is the information housed?
☒ Department-owned equipment
☐ FEDRAMP-certified cloud
☐ Other Federal agency equipment or cloud
☐ Other

- If you did not select "Department-owned equipment," please specify.
Click here to enter text.

(e) What process is used to determine if the information is accurate?
Exchange 15.x does not verify accuracy of PII. Exchange 15.x only serves as a repository of the information collected by the governing authorities.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?
Exchange 15.x does not maintain/administer PII. Exchange 15.x only serves as a repository of the information. The onus to ensure the information is current is on the originator of the collection of information.

(g) Does the system use information from commercial sources? Is the information publicly available?
Exchange 15.x does not collect information from commercial or publicly available information.

(h) Is notice provided to the individual prior to the collection of his or her information?
The owning office/bureau is responsible for notifying an individual prior to collecting their information.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☐Yes ☒No

- If yes, how do individuals grant consent?
Click here to enter text.

- If no, why are individuals not allowed to provide consent?

The user's consent to use their PII is the responsibility of the owning office/bureau.

(j) How did privacy concerns influence the determination of what information would be collected by the system?

OpenNet Email is classified as Sensitive But Unclassified (SBU) due to the content of private information that users may include in their communications. Rules of Behavior have been established for end users to follow to ensure the laws and regulations governing the use of Exchange are being adhered to.

5. Use of information

(a) What is/are the intended use(s) for the information?

Uses of the information (contained in emails) are dependent upon the business needs of the bureau/office gathering the data.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

Yes.

(c) Does the system analyze the information stored in it? ☐Yes ☒No

If yes:

(1) What types of methods are used to analyze the information?

(2) Does the analysis result in new information?

Click here to enter text.

(3) Will the new information be placed in the individual's record? ☐Yes ☐No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it? ☐Yes ☐No

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.
Recipients of the information include approved DOS government and contracting personnel, various federal agencies, U.S. citizens and non-U.S. persons

(b) What information will be shared?
Information that is pertinent to support DOS business processes and guidelines. For example, an e-mail address (considered PII) is usually present on the To: or CC: lines of every e-mail sent.

(c) What is the purpose for sharing the information?
Information is shared to support DOS business requirements and varies by email sender and bureau.

(d) The information to be shared is transmitted or disclosed by what methods?
The information to be shared is transmitted via a secure email gateway.

(e) What safeguards are in place for each internal or external sharing arrangement?
The information that governing authorities communicate through email is safeguarded behind the DOS network and firewall preventing unauthorized access.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?
Privacy concerns such as password sharing or misuse of DOS email system is addressed through training and acknowledgement that users of the system comply with this requirement. Non-compliance is addressed through documented procedures to secure privacy of information.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?
Individuals wishing to access and amend Privacy Act covered information maintained by Exchange should contact the office/bureau that originally collected it.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?
☒Yes ☐No

If yes, explain the procedures.
Procedures vary by the mission of the office or bureau. Individuals should contact the office or bureau responsible for the initial collection of their information for redress purposes.
If no, explain why not.

(c) By what means are individuals notified of the procedures to correct their information?

-The office/bureau collecting the PII provides the procedures or other mechanisms to correct user's information.

8. Security Controls

(a) How is the information in the system secured?

Information in the system is secured through multiple layers of security, including identification (ID) badge access to buildings and user accounts configuration authentication requirements to the network (e.g., passwords and personal identification verification (PIV) cards), and role-based access through Active Directory (AD) group membership to control individual access based on authorized roles and responsibilities.

(b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.

PII communicated through email is accessible to cleared DOS direct hire and contractor employees. All access is enforced by user profiles according to the principle of the least privilege and the concept of separation of duties. In addition, there are monitoring tools in place, such as the System Center Operations Manager (SCOM), to record proposed security violations in system logs, including unauthorized access, and send alerts to administrators. Email Division roles with access to Exchange are Exchange Engineers, Email Operations Administrators, Email System Administrators and the End user.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

Email utilizes the SCOM tool to monitor all systems and provide alerts when needed. The system also provides a detailed recording of access via log files detailing when and who accesses the email system. This information is saved per DS data retention requirements, and provided to DS as needed.

(d) Explain the privacy training provided to authorized users of the system.

Both Government and Contracting staff are required to undergo annual PS800 Cybersecurity Awareness training and PA459 Protecting Personally Identifiable Information privacy training. If this requirement is not met, the individual will be locked out of the system.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒Yes ☐No

If yes, please explain.

Yes, data is encrypted per FIPS 140-2 guidelines.

(f) How were the security measures above influenced by the type of information collected?

Due to the nature and content of DOS business operations, system and security measures such as user authentication are in place to safeguard against unauthorized access or compromise to the system.

9. Data Access

(a) Who has access to data in the system?
Only Department approved government employees or supporting contractors.

(b) How is access to data in the system determined?
Access to system data is determined by security and support requirements.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.
Access to system data is restricted based on the employee's specific role.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?
Access control is implemented via the secure network; authentication to system is granted via AD individual and group role membership. In addition, security tools are in place to proactively monitor subject system(s).